



Inglourious Hackerds Targeting Web Clients

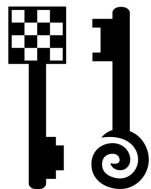


www.tehtri-security.com



INGLOURIOUS HACKERDS

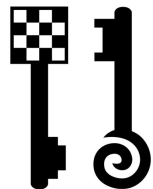
TARGETING WEB CLIENTS



Speaker

- Laurent OUDOT

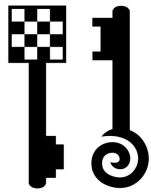
- Founder & CEO of TEHTRI-Security
- Senior Security Expert
 - When ? 15 years of IT Security
 - What ? Hardening, Penetration Tests...
 - Where ? On networks and systems of highly sensitive places:
 - *French Nuclear Warhead Program, United Nations, French Ministry of Defense...*
- Research on defensive & offensive technologies
 - *Past: Member of the Steering Committee of the Honeynet Alliance...*
 - Frequent presenter and instructor at computer security and academic conferences like SyScan SG-CN, Cansecwest, Pacsec, BlackHat USA-DC-AbuDhabi-Asia-Europe, HITB Dubai-Amsterdam-Malaysia, US DoD/US DoE, Defcon, Hope, Honeynet, PH-Neutral, Hack.LU...



About TEHTRI-Security

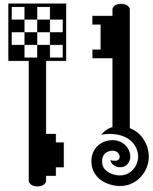
- Company created in April 2010
- Cutting-edge technologies
 - Advanced & Technical Consulting
 - Penetration Tests / Audits...
 - Fighting Information Leaks, Counter-Intelligence...
- Worldwide:
 - Conferences, Training, Consulting
 - USA, Canada, Lebanon, United Arab Emirates, Singapore, Netherlands, China, Malaysia, France...
 - Press/Media     
- >35 public security advisories (12 months)
 - Pentesting devices & Applications → 0days...





Introduction

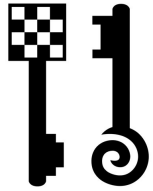
- Goal:
 - To analyze some techniques used by *inglourious hackerds*, targeting web clients
 - To think about solutions
- Target audience:
 - White hats, to fight against Cybercrime, Business Intelligence, Information Warfare
- Notice:
 - Legal Issues: we remind you to carefully respect the laws in your country before applying some techniques shown in this presentation
 - Limitation: this is an almost 1 hour only talk. We won't be able to cover all the related subjects. Contact us for more...



Plan

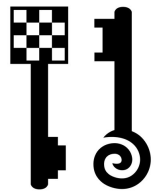
Inglourious Hackerds, Targeting Web Clients

- 1 – Global Overview
- 2 – Finding vulnerabilities
- 3 – Attacking Web Clients
- 4 – Conclusions



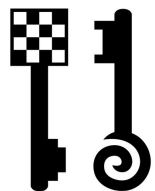
Let's have a look at the theory and at some concepts related to attacks against web clients

I. GLOBAL OVERVIEW



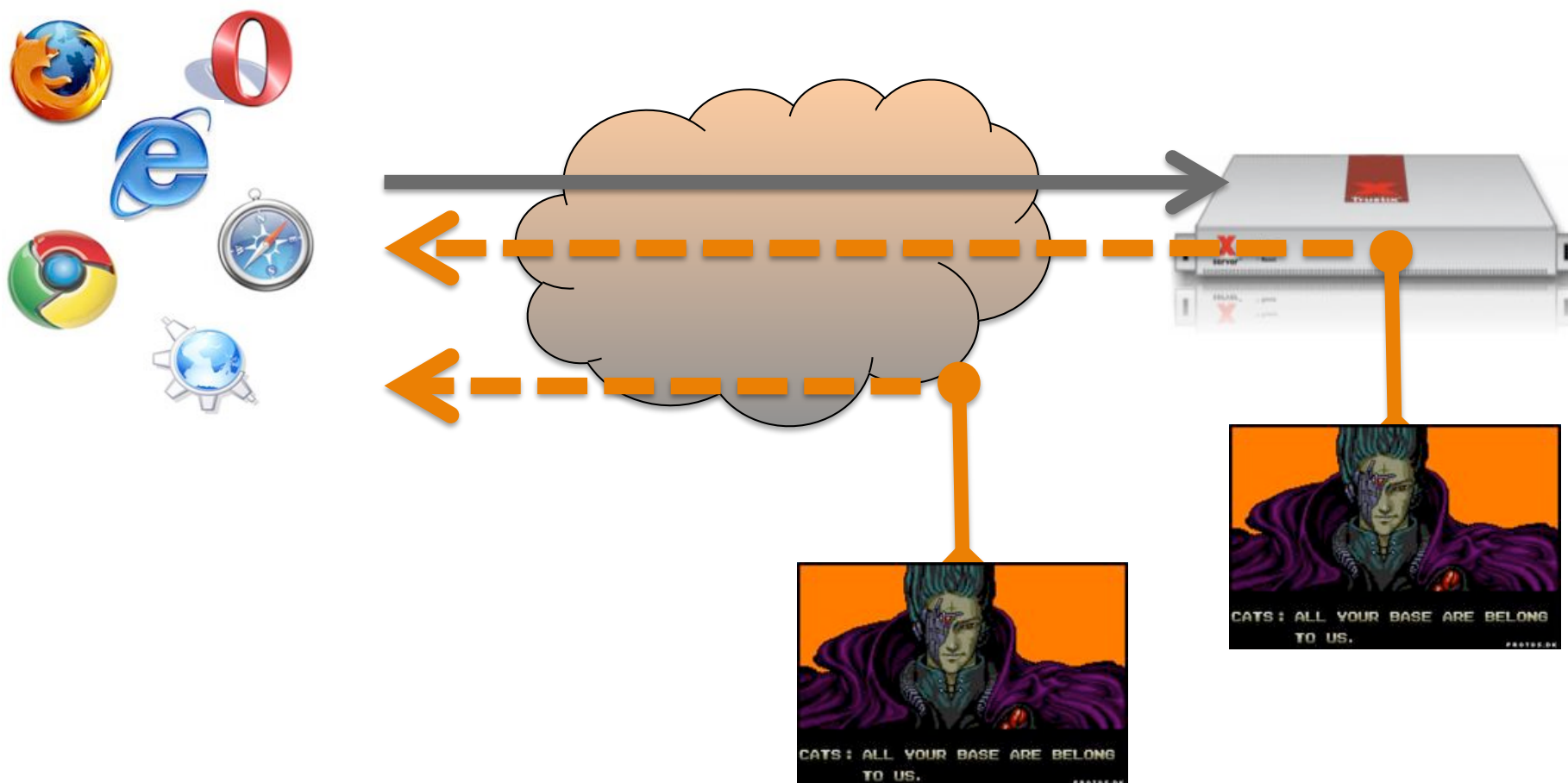
Battlefield: Web Hacking

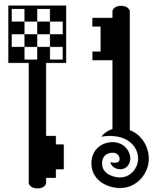
- Web targets (standard aspects)
 - Web Clients (browsers)
 - Client-side attacks
 - “Human” interaction (at least the beginning)
 - Web Servers (services)
 - Direct attacks
 - Technical interaction
- In this presentation, we'll focus on attacks against **web browsers**, and how inglorious hackerds try to play hard against their targets



Targeting Web Clients

- Evil responses (Server or MITM)





Example: Wifi threats



Home



Coffee/Bars



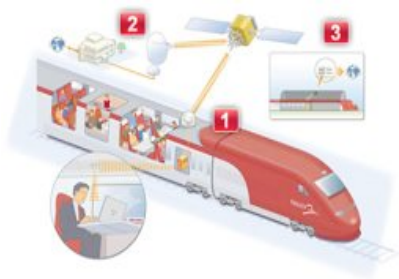
Restaurants



Hotels



Corporate...



Trains



Planes

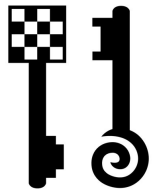


Bus

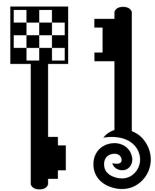


Taxis / Cars



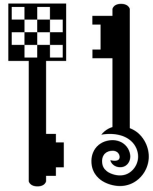


2. FINDING VULNERABILITIES



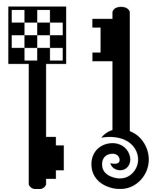
Finding vulnerabilities

- Reverse
- Fuzzing
- Analyzing behavior (Logs, Sniffing...)
- Audit
- Pentest
- ...



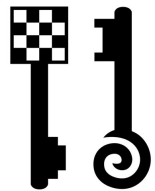
Fuzzing

- Sounds easy
- Not that easy
 - Random fuzzing → Sharp fuzzing
- Example with handled devices
 - Special HTML code supported (URL)
 - `<a href="sms:"`
 - `<a href="tel:"`
 - ...



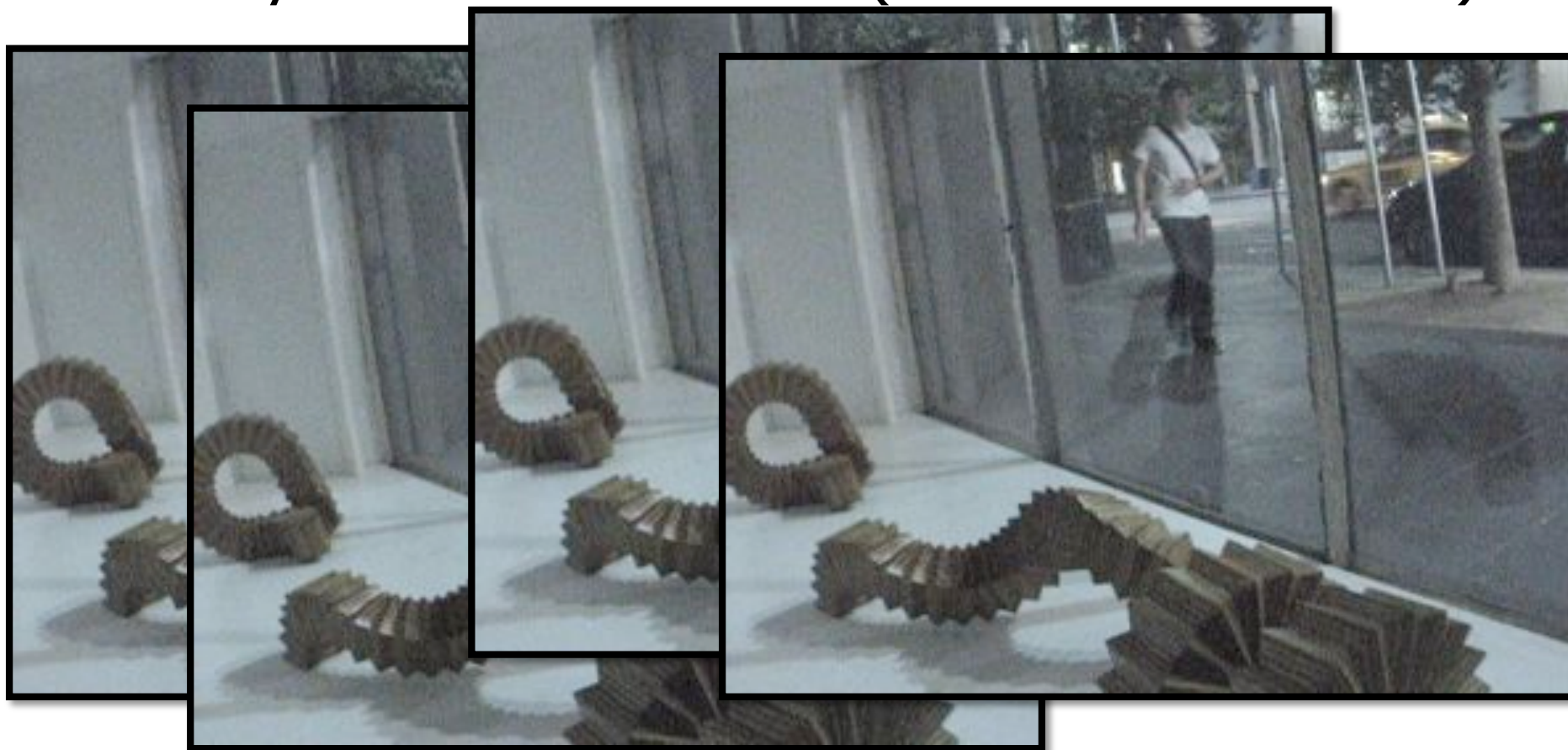
So cool embedded software... But no security audit, No penetration tests, Bad hardening, Bad architecture...

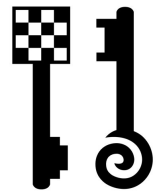
IP CAMERA



Finding 0days in devices

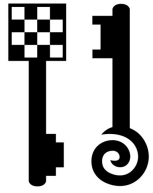
- E.g.: TEHTRI-Security found a 0day against a widely used IP Camera (Web Surveillance)



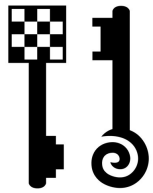


Abusing remote Camera Networks





IPHONE PERSONAL HOTSPOT

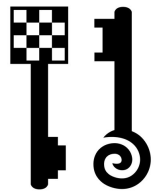


iPhone Personal Hotspot



- New feature
- iPhone 4 + iOS 4.3 → iPhone = Hotspot
 - WPA2 PSK on ap0
 - Read more on <http://blog.tehtri-security.com/2011/03/about-iphone-ios43-personal-hotspot.html>

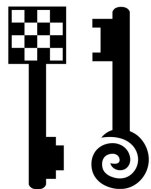




iPhone Personal Hotspot: **VULN**



- Platform: iPhone 4
- Operating System $\geq$ iOS 4.3 (8F190)
- Application: `com.apple.wifi.hostapd`
- Impact for customers: Low (?)
 - “Personal Hotspot” uses a passphrase to protect the WPA2 Personal wireless hotspot created. A WPA PSK is derived from it.
 - While processing those functions, the iPhone writes the passphrase in clear text in the console of the iPhone device.
 - This area is readable by all local processes through the official Apple API.



Example of attack result



- Here is the list of things written in clear text through the console:
 - The Group Master Key + the Group Transient Key,
 - The PSK + the passphrase.

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.357484: PSK
(ASCII passphrase) - hexdump_ascii(len=10):

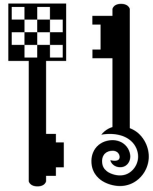
Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : **66 61 63 65 74 73**
31 34 36 37 **facets1467**

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.733079: PSK
(from passphrase) - hexdump(len=32): **cf f6 0d 2a 1a a2 d8 29 6d 58 cc 6f**
49 55 34 47 22 b7 9c 5c 76 86 be 17 57 b0 d3 5c 6e ad 2a 65

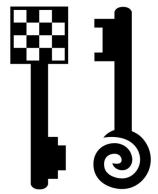
Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.870472:
WPA: group state machine entering state **GTK_INIT** (VLAN-ID 0)

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.870522: **GMK**
- hexdump(len=32): **f9 69 7e c4 d1 fa 41 10 e2 b9 a1 78 0e 50 fa 47 5b 18 4a**
86 75 8d a1 64 c7 c9 fc 7d b2 98 d5 b3

Mar 5 01:23:24 unknown com.apple.wifi.hostapd[79] : 1299338601.870580: **GTK**
- hexdump(len=16): **8d 3f 27 be 0c 21 e2 5e fb 92 fb 15 b2 69 eb cd**

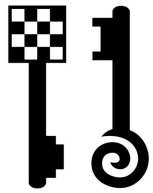


IPHONE APPLICATIONS



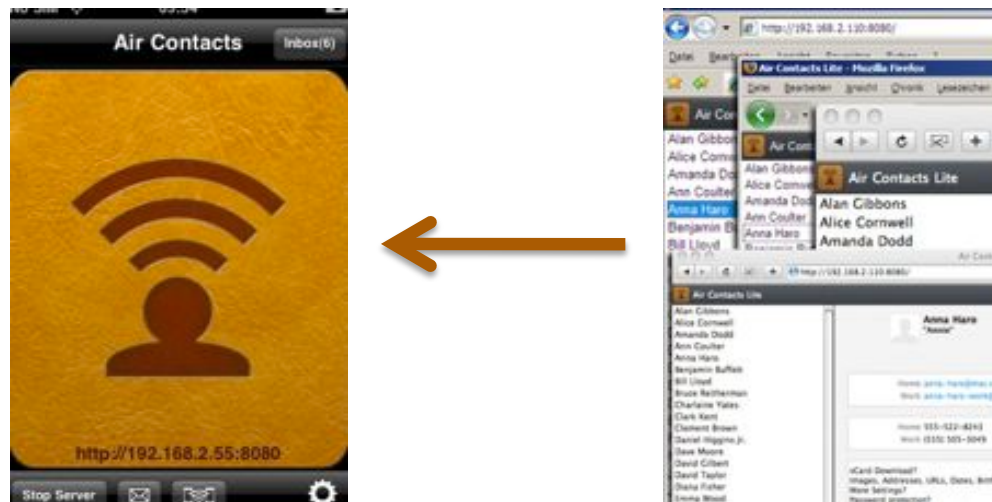
What about iPhone APP Security ?

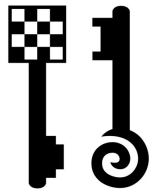
- While Android market is said to contain many dangerous applications, Apple App Store forces developers to follow strict coding style
- Applications are supposed to be well coded with (almost) no vulnerability



Example of security issues

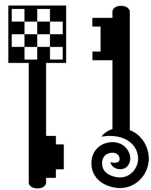
- Example of security issues against an application from the Apple Store
- Name: « Air Contacts »
- Goal: share contacts between your iPhone and local Wifi browsers



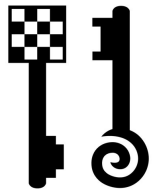


Example of 0day (DoS)

- By forging some HTTP requests, one can crash the remote Application
 - Example with Empty field
 - GET /personimage?i_recId=
 - 0day Remote: XSRF, 0day Local Wifi: Direct HTTP
 - Crash result
 - Hardware Model: iPhone3,1
 - Process: Air Contacts Lite [3115]
 - Identifier: Air Contacts Lite
 - Code Type: ARM (Native)
 - Parent Process: launchd [1]
 - OS Version: iPhone OS 4.3 (8F190)
 - Report Version: 104
 - Exception Type: EXC_BAD_ACCESS (SIGBUS)
 - Exception Codes: KERN_PROTECTION_FAILURE at 0x00000028
 - Crashed Thread: 0

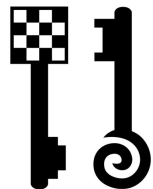


3. ATTACKING WEB CLIENTS



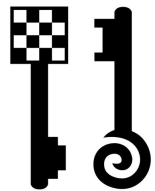
RTFM: RFC

- RFC 2396 « Uniform Resource Identifiers (URI): Generic Syntax »
- RFC 2616 « Hypertext Transfer Protocol -- HTTP/1.1 »
 - The HTTP protocol does not place any a priori limit on the length of a URI. Servers MUST be able to handle the URI of any resource they serve, and SHOULD be able to handle URIs of unbounded length if they provide GET-based forms that could generate such URIs.
 - A server SHOULD return 414 (Request-URI Too Long) status if a URI is longer than the server can handle (see section 10.4.15).



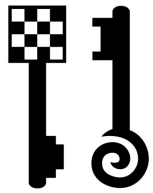
Exploit ?

- According to RFC: no limit to the size of a URI
- Reality: practical limits on the available resources
 - Solution: limitations fixed by vendors
 - Example:
 - <http://support.microsoft.com/kb/208427>
 - Maximum URL length is 2,083 characters in Internet Explorer
- Special case: mobile devices
 - Limited resources
 - Special analysis of HTML
 - Dynamic interpretation of phone numbers, dates, etc



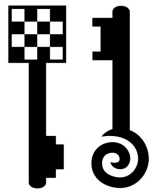
Example of Security Issue

- Handled devices
- Analyzing HTML content
 - Make decisions about how to process a link based on its structure and makeup
 - Designed with typical/average length URIs
 - Consists of walking through the URI several times, performing comparisons and trying to extract things such as email addresses or phone numbers
 - Then it might need to launch appropriate external application (email composer, sms editor, etc)

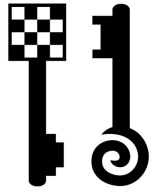


What if ?

- Security issue
 - Extremely long URI provided with evil links
 - Parsing takes up a considerable amount of resources (typically, memory and CPU cycles) and the web client is unresponsive while it waits for the parsing to complete
- Watchdog mechanism detects that a process is stuck or otherwise unresponsive
- Error message displayed and/or crash
 - Sometimes it's not descriptive from an end user's perspective but it is accurately stating what has happened
 - The web client process or other processes or the device, might terminate because it has stalled

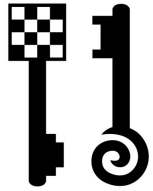


EXPLOIT(S) ?



APPLE PRODUCTS

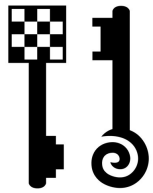




Security Issue Found



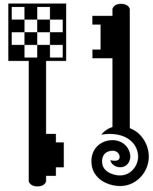
- Stack overflow in CFNetwork's URL handling code
 - Low layer found in many Apple products
- Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution



Products affected



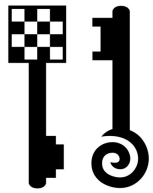
- Safari on Windows
- Safari on Mac OS X
- CFNetwork on iPod
- CFNetwork on iPhone



Vendor responses



- Discussions
 - First advisories in June/July 2010
- Patches
 - Improved memory handling
- CVE-2010-1752
 - iPod
 - iPhone (patch with iOS 4)
 - Safari Windows
 - Safari MacOSX and MacOSX Server

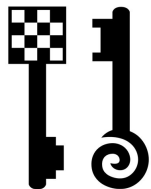


Another trick



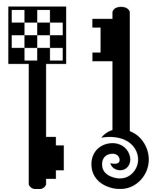
- iPad Advisory: TEHTRI-SA-2010-026
 - Watchdog crash due to low memory conditions (not related to CFNetwork)
 - Cannot be exploited to execute arbitrary code. Fixed in a future software update.





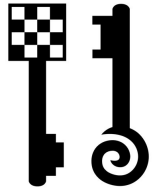
E.g. Safari on Windows

- Sun Feb 22 02:03:36.570 2010 (UTC + 2:00): (e70.a84):
Stack overflow - code c00000fd (first chance)
- First chance exceptions are reported before any exception handling. This exception may be expected and handled.
- eax=00032000 ebx=0c3e0020 ecx=00000000 edx=027b2060
esi=0c3e0020 edi=055d4aae eip=017a80d7 esp=0012f10c
ebp=0012f12c iopl=0 nv up ei pl nz na pe nc cs=001b
ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
- Loading symbols for 01750000 C:\Program Files\....
\Apple\Apple Application Support**CFNetwork.dll**
- CFNetwork!**CFURLProtocolSendDidFinishLoadingCallback**
+0x6056: 017a80d7 8500 test dword ptr [eax],eax ds:
0023:00032000=00000000
- Loading symbols for 01f90000 C:\Program Files\....
\Apple\Apple Application Support**WebKit.dll**



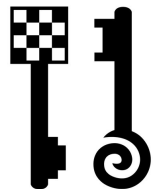
E.g. Safari on MacOSX

```
▪ Process: Safari [3254]
▪ Path: /Applications/Safari.app/Contents/MacOS/Safari
▪ Identifier: com.apple.Safari
▪ Version: 5.0.2 (6533.18.5)
▪ Build Info: WebBrowser-75331805~1
▪ Code Type: X86-64 (Native)
▪ Parent Process: launchd [3178]
▪ OS Version: Mac OS X 10.6.4 (10F569)
▪ Crashes Since Last Report: 1739
▪ Exception Type: EXC_BAD_ACCESS (SIGSEGV)
▪ Exception Codes: KERN_PROTECTION_FAILURE at 0x00007fff5df61b38
▪ Crashed Thread: 0 Dispatch queue: com.apple.main-thread
...
▪ Thread 0 Crashed: Dispatch queue: com.apple.main-thread
▪ 0 com.apple.CFNetwork 0x00007fff859a9686 URLResponse::copySuggestedFilename() + 806
▪ 1 com.apple.Foundation 0x00007fff80e7c352 -[NSURLResponse suggestedFilename] + 31
▪ 2 com.apple.WebCore 0x00007fff84d0d26b WebCore::ResourceResponse::platformLazyInit() + 475
▪ 3 com.apple.WebCore 0x00007fff84d86b91 WebCore::ResourceResponseBase::statusCode() const + 17
▪ 4 com.apple.WebCore 0x00007fff84d91e25
WebCore::ApplicationCacheHost::maybeLoadFallbackForResponse(WebCore::ResourceLoader*, WebCore::ResourceResponse const&) + 37
▪ 5 com.apple.WebCore 0x00007fff84d91d43 WebCore::ResourceLoader::didReceiveResponse
(WebCore::ResourceHandle*, WebCore::ResourceResponse const&) + 67
...
▪ Thread 0 crashed with X86 Thread State (64-bit):
▪ rax: 0x0000000001c9c390 rbx: 0x00000001194e43b8 rcx: 0x00007fff7118e3e0 rdx: 0x0000000001c9c390
▪ rdi: 0x000000012c089000 rsi: 0x00007fff5df61b40 rbp: 0x00007fff5fbfdf50 rsp: 0x00007fff5df61b40
▪ r8: 0x00007fff85a0fd3e r9: 0x0000000000000000 r10: 0x00000001008aa750 r11: 0x00007fff5fbfde80
▪ r12: 0x000000012c089000 r13: 0x0000000117601de0 r14: 0x0000000100af4900 r15: 0x00007fff84d91d00
▪ rip: 0x00007fff859a9686 rfl: 0x0000000000010202 cr2: 0x00007fff5df61b38
```



RIM PRODUCTS

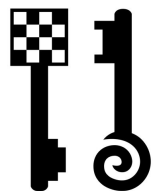




Security Issue Found



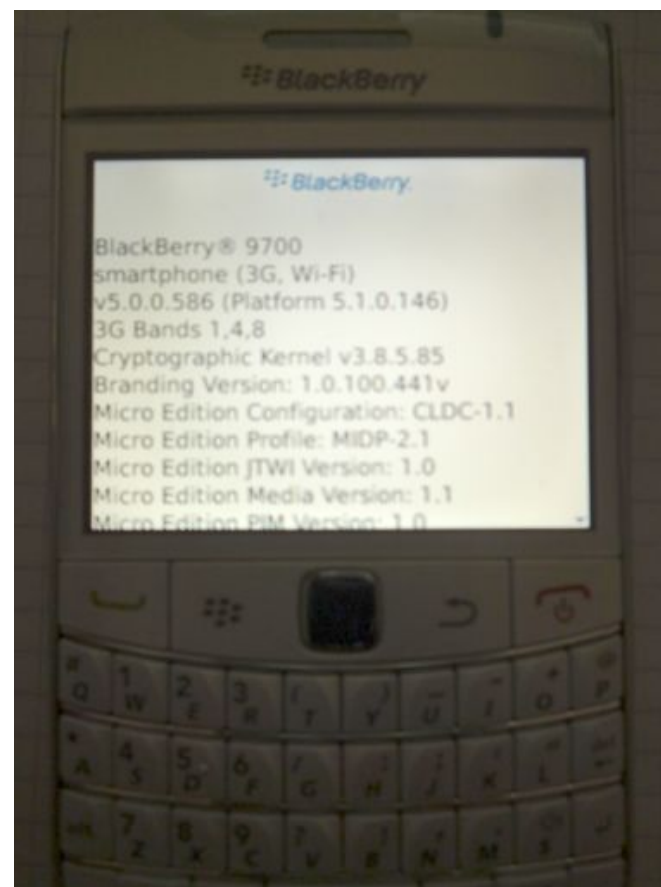
- Maliciously crafted web page viewed by a vulnerable BlackBerry → the browser application becomes unresponsive
- The BlackBerry device subsequently terminates the browser, and the browser eventually restarts and displays an error message.
- Successful exploitation of this issue relies on the user viewing the maliciously crafted web page on a device running the affected BlackBerry Device Software.
- The impact is limited to a partial Denial of Service (DoS) in the browser application in use on the BlackBerry device

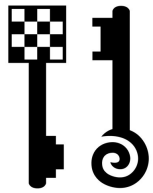


Products affected



- The issue affects the BlackBerry browser application of the following software versions:
- BlackBerry Device Software versions earlier than 6.0.0
- Hotspot Browser on BlackBerry
 - "BlackBerry9700/5.0.0.586 Profile/MIDP-2.1 Configuration/CLDC-1.1 VendorID/100"

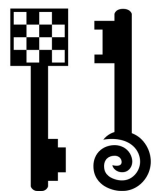




Vendor responses



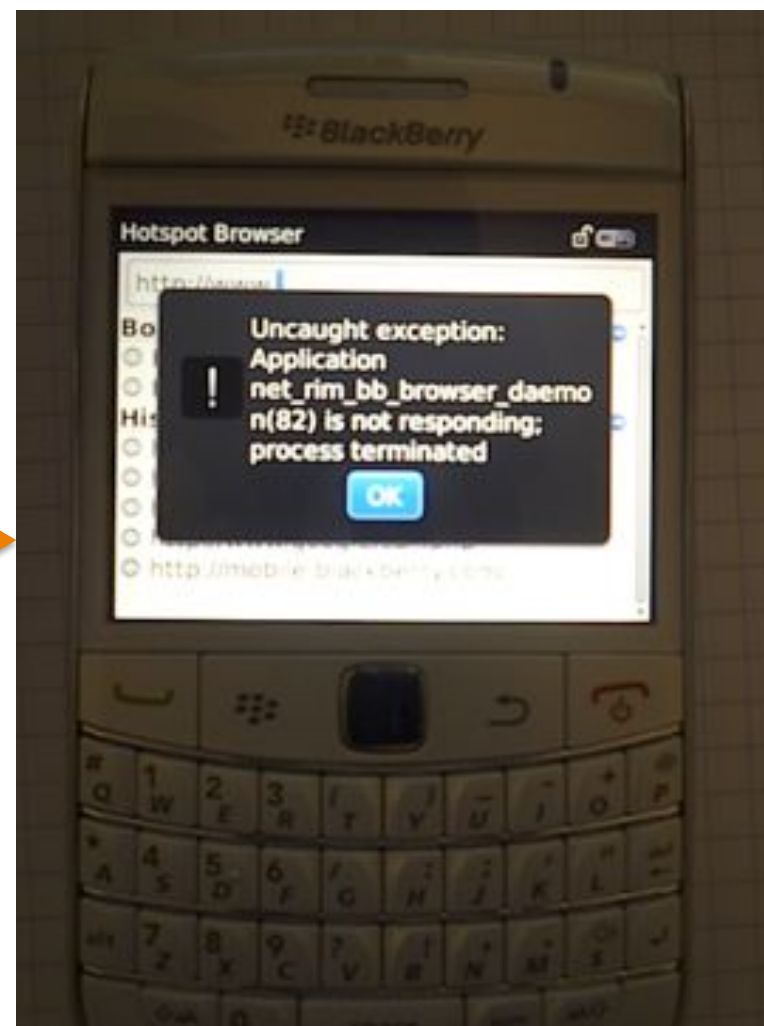
- RIM has issued a software update that resolves this issue in BlackBerry Device Software versions later than 5.0.0. BlackBerry Device Software version 4.7.0 and earlier is unsupported, and versions later than 6.0.0 are unaffected.
- BlackBerry Security Response answered to any of our emails in a really short period of time
- Speed++
 - They handled the security issues & did a great investigation
 - Development of a fix very quickly for future releases + Patch for old products
- CVSS: 5/10

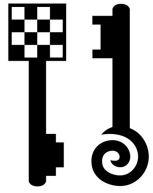


Technical details

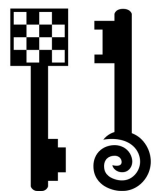


- CVE-2010-2599
- TEHTRI-SA-2010-027





QUICK BLACKBERRY SECURITY CHECK

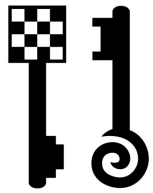


Quick BB Security Check



- Here @SyScan, first time announced during a conference
 - Quick Blackberry Security Check
 - tehtris.com/bbcheck
 - Was put online one month before SyScan
 - Quick security check
 - Known vulnerability ?

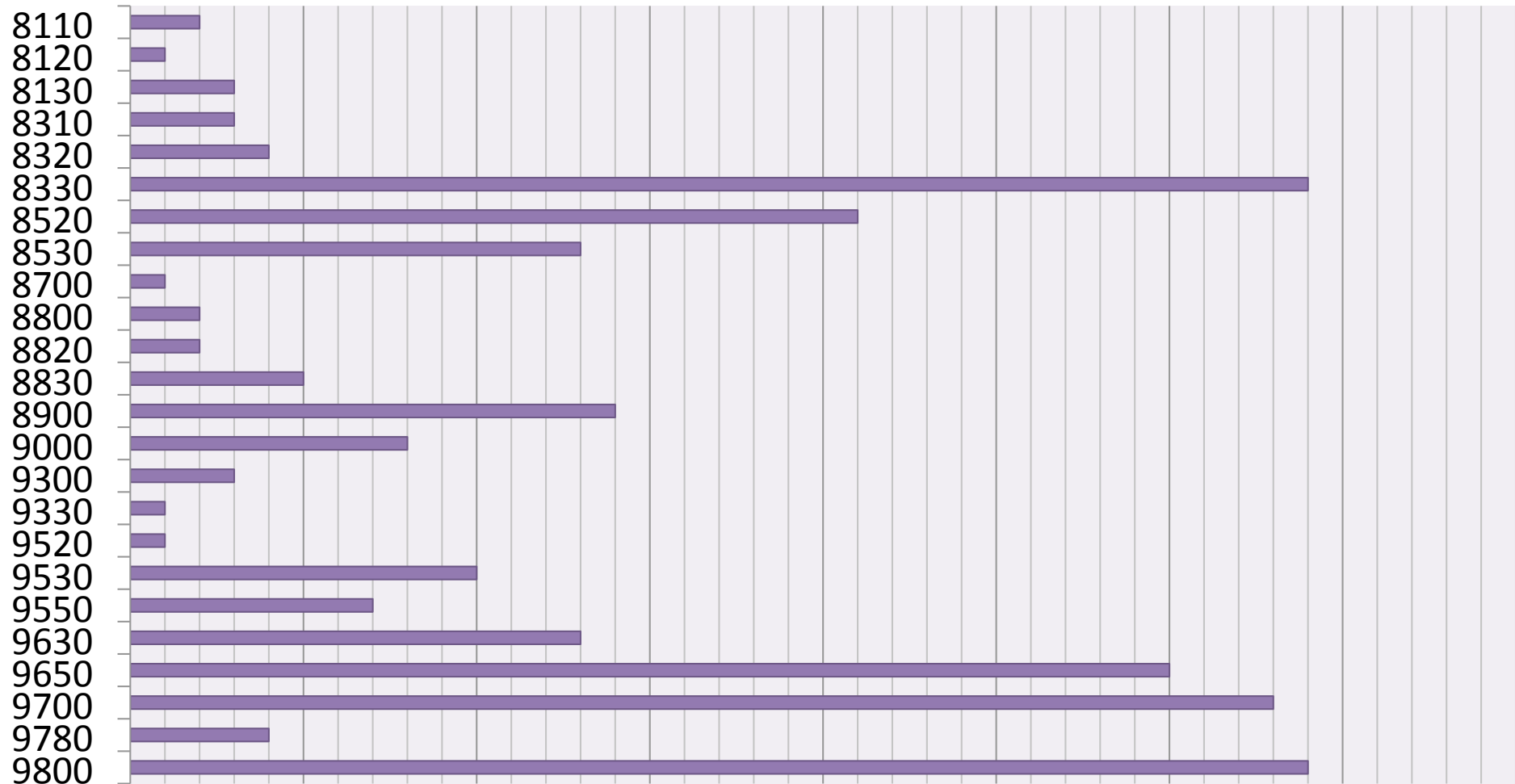


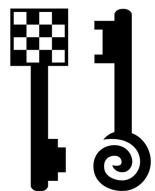


BBCheck: Statistics for Platforms



BlackBerry Platforms

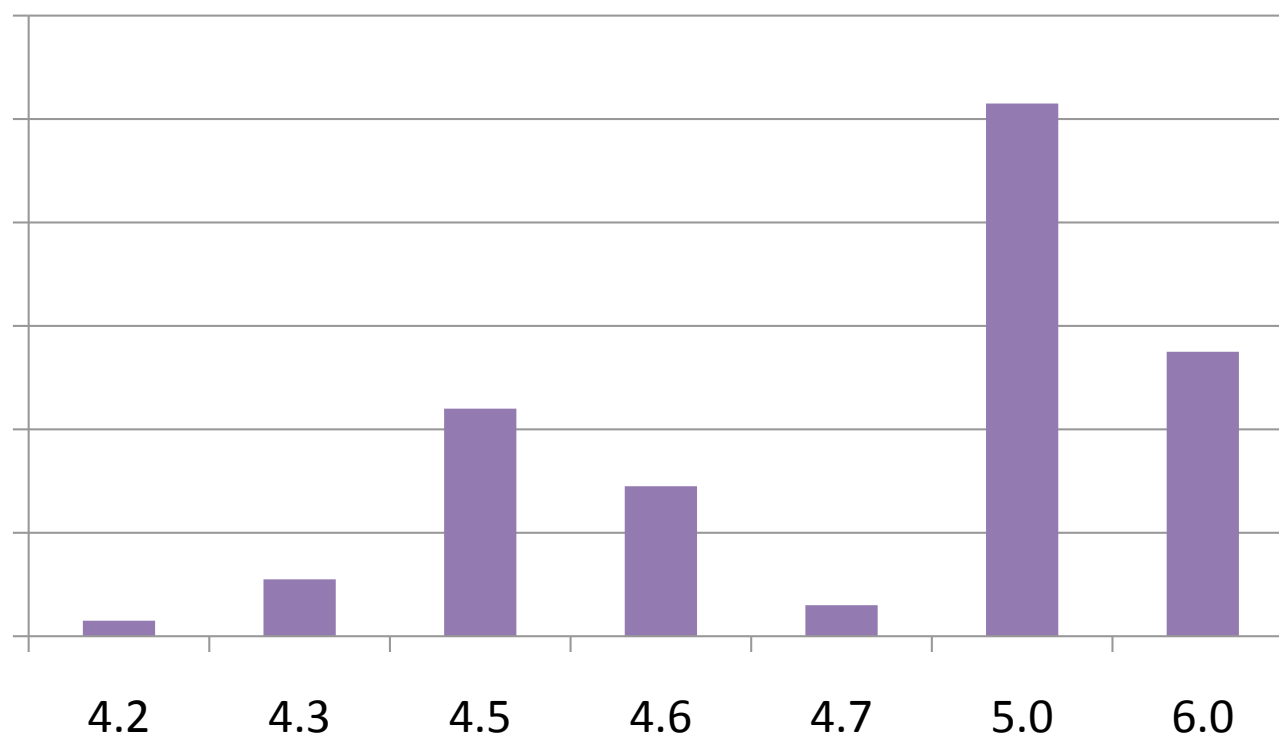


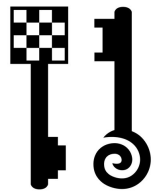


BBCheck: Statistics for Versions



BlackBerry Versions (from 4.2.* to 6.0.*)

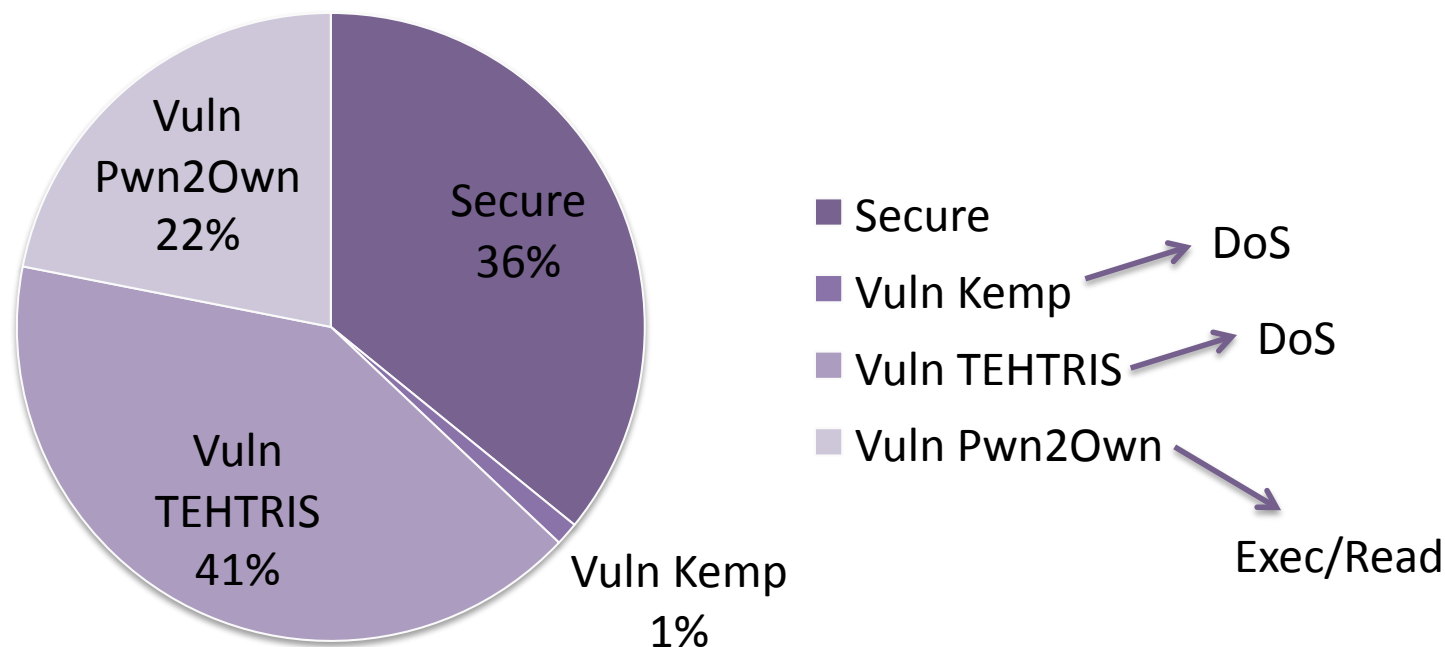


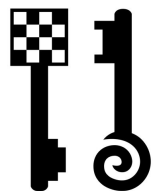


BBCheck: Statistics for Security



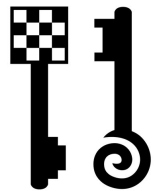
Are your blackberry device vulnerable ?





GOOGLE PRODUCTS

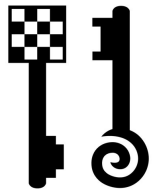




Security Issue Found

- Overflow against application Browser on Android with large input from the web
- Overflow against application Gmail on Android with large input from the web

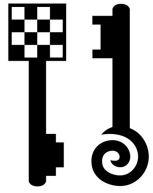
e.g: « Gmail is prone to a vulnerability after being launched by Browser trying to handle some web pages that would contain specific evil code. »



Products affected

android

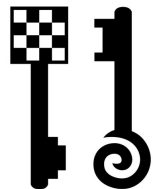
- Firmware tested: 1.5
- Kernel version tested: 2.6.27
- User-Agent tested:
« Mozilla/5.0 (Linux; U; Android 1.5; en-us;
GT-I5700 Build/CUPCAKE)
AppleWebKit/528.5+ (KHTML, like Gecko)
Version/3.1.2 Mobile Safari/525.20.1 »
- Name: Gmail (com.google.android.gm)
Activity: Compose (application Gmail)
- Name: Browser (com.android.browser)



Vendor responses

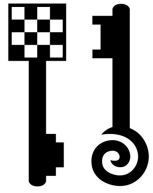
ANDROID

- « Traditionally, we do not consider local denial of service attacks of this kind to be security bugs. »
- No patch needed 😊



Proof of Concept #1

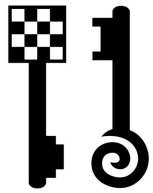
Shown during SyScan
Singapore 2011 only



Technical details #1

android

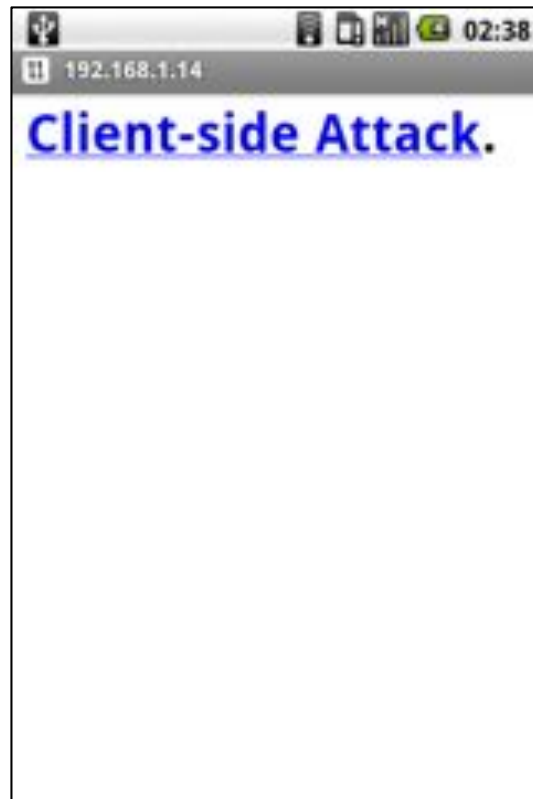
Shown during SyScan
Singapore 2011 only

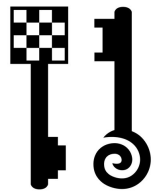


Screenshots #1

ANDROID

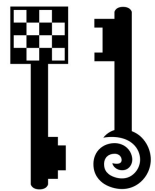
- Overflow against application Browser on Android with large input from the web





Proof of Concept #2

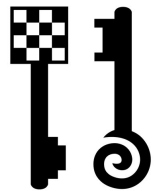
Shown during SyScan
Singapore 2011 only



Technical details #2

android

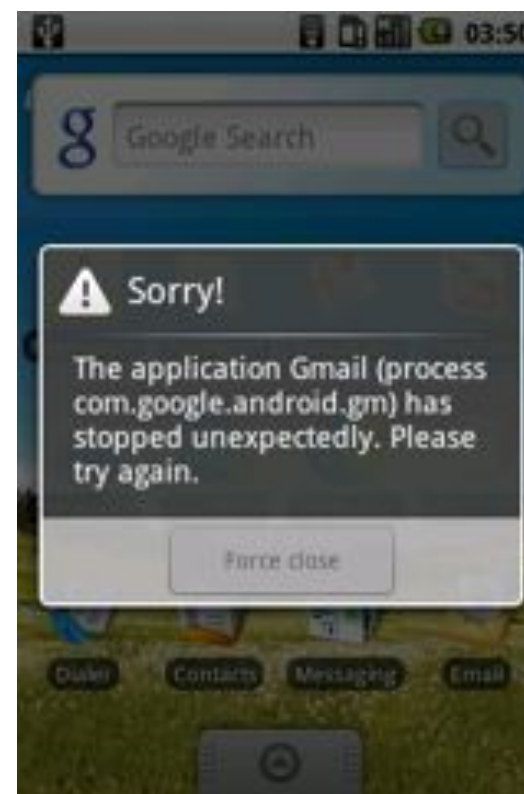
Shown during SyScan
Singapore 2011 only

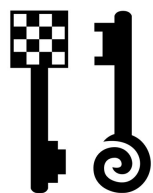


Screenshots #2

ANDROID

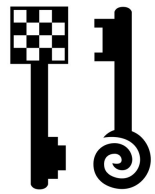
- Overflow against application Gmail on Android with large input from the web





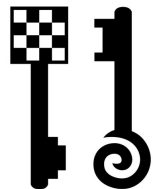
Found by TEHTRI-Security [2010]

Vendor / Product	Tool / Version	Reference	Patch
Apple / iPod	iOS 2.1-3.1.3 for iPod touch (2nd generation) and later	CVE-2010-1752	Patched (iOS4)
Apple / iPhone	iOS 2.0-3.1.3 for iPhone3G & later	CVE-2010-1752	Patched (iOS4)
Apple / Safari Windows	Safari 5.0.3 and Safari 4.1.3 on Windows 7, Vista, XP SP2 or later	CVE-2010-1752	Patched
Apple / Mac OS X	CFNetwork on Mac OS X v10.5.8, Mac OS X v10.6 through v10.6.4 (idem for Mac OS X Server)	CVE-2010-1752	Patched
Apple / iPad	Any version (but no exec)	TEHTRIS 2010 26	Under construction
RIM / BlackBerry	BlackBerry Device Software versions later than 5.0.0	CVE-2010-2599	Patched
HTC Windows	...	?	?
Google Android	Browser & Gmail	?	?



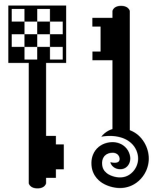
Thoughts / Security Updates

- Our return of experience (might be different for you), about what we saw on the battlefield:
 - On blackberry devices (power organized)
 - Administrators (BES...) don't like to update
 - Users don't really know how to update
 - On iPhone devices (power to people)
 - Administrators cannot handle the updates
 - Most of the time, end users will handle updates by themselves through the iTunes reminder during each sync (unless devices are JailBroken)



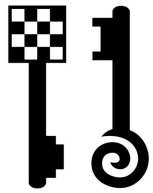
Is that a security threat ?

- Those attacks can be used by combining different techniques
 - Mail: Imagine evil links sent by email directly with pointers to bad servers
 - MITM: Imagine a wireless hotspot with someone running all those exploits for any vulnerable devices?
 - Crash of vulnerable devices... (massive pwnd/DoS)
 - You could also add another trick:
 - 1st you crash the clients,
 - 2nd you display a fake security web page for phishing, etc
 - » *Vendor message: your device just crashed and we need to re-enroll your account for your security, please fill in the form...*
- Other vendors? 😊



Do you still prefer to deploy web products without stressing them with IT security technical pentesters?

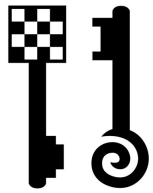
4. CONCLUSIONS



Situation



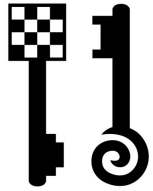
- Beyond the technical world, lot of external problems
 - Some believe that products are secured by default
 - But IT infrastructures get more and more complex
 - And we all face money and speed issues...
- So that, many products are used without being stressed or tested by skilled consultants
 - Cell phones, VOIP phones, IP Camera...
 - Vulnerabilities (0days) & Offensive concepts
 - Low costs behaviors can cost a lot



Conclusion



- Behavior
 - Being certified → Feeling secure
 - Being certified ≠ Being secure
 - Are your enemies “ethical hackers” ?
- What should be done?
 - You saw how easy it was to found multiple web vulnerabilities on widely used products
 - Hardening + (real) Pentest + Analysis
 - Before buying stuff + before & after deployment...



THANKS !

- SyScan Crew & COSEINC folks
- RIM Company (Kymberlee Price, Adrian Stone, Mark Long, Michael McCallum...)
- Apple Folks (@product-security: Jeffrey, Matt, Geoff, Mihaela...)



This is not a game.

Take care.Thanks.

<http://www.tehtri-security.com>

[Twitter | Facebook | RSS | Blog ...]

web (at) tehtri-security (dot) com

Twitter: @tehtris